- Fault Tolerance

FLEX 19
1S.D

Dependable systems

Dependability: a definition

A system is ***designed*** to provide a certain service. Dependability is the ability of a system to deliver a specified service.

In particular:

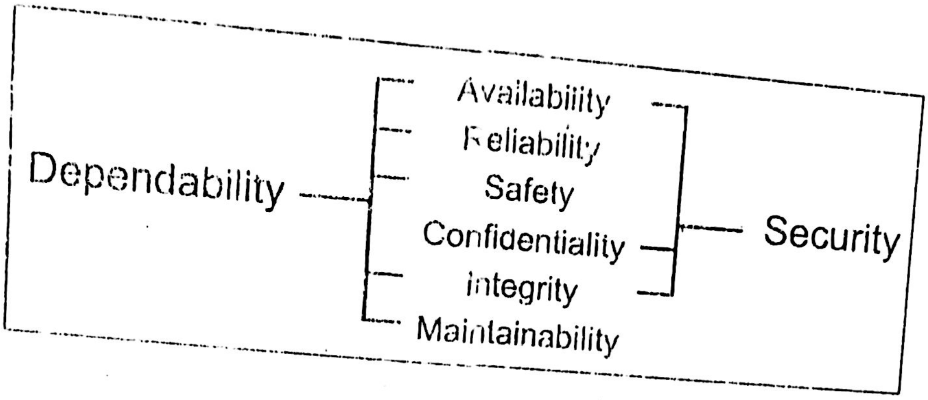
Dependability is "that property of a computer system such that reliance can justifiably be placed on the service it delivers" If the system stops delivering the intended service, we call this a failure.

Dependability attributes

Dependability is a concept that encompasses multiple properties:

- **Availability**
  readiness for correct service
- **Reliability**
  continuity of correct service
- **Safety**
  absence of catastrophic consequences on the user(s) and the environment
- **Confidentiality**
  the absence of unauthorized disclosure of information
- **Integrity**
  absence of improper system alterations
- **Maintainability**
  ability to undergo modifications and repairs

➢ Dependability properties can be measured in terms of probability



What is a system?

System: entity that interacts with other entities, i.e., other systems, including

- hardware.
- networks,
- operating systems software,
- application software,
- humans, and
- the physical world with its natural phenomena.

These other systems are the environment of the given system.

The **system boundary** is the common frontier between the system and its environment.

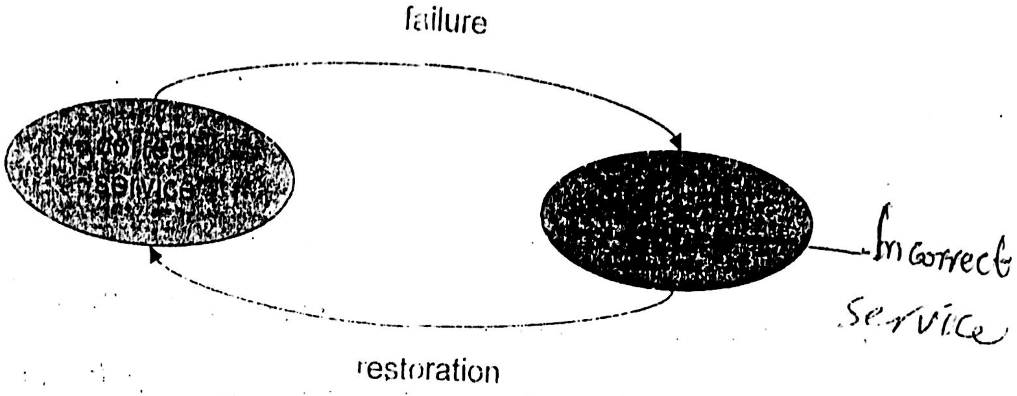
Fundamental properties of a system:
functionality, performance, dependability and security, and cost.

Threats to Dependability: Failures, Errors and Faults

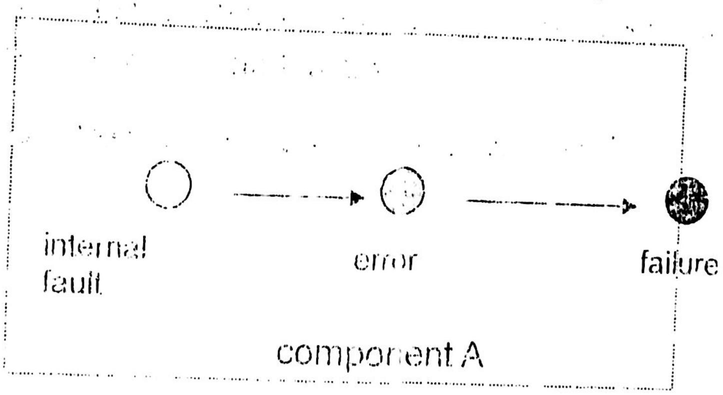
Correct service is delivered when the service implements the system function.

A service failure, often abbreviated failure, is an event that occurs when the delivered service deviates from correct service. A service fails either because it does not comply with the functional specification,or because this specification did not adequately describe the system function.

Failure is a transition from correct service to incorrect service, Restoration is the transition from incorrect service to correct service.



Threats to Dependability: Failures, Errors and Faults



A fault causes an error in the internal state of the system. The error causes the system to fail

Partial failure: Services implementing the functions may leave the system in a degraded mode that still offers a subset of needed services to the user. The specification may identify several such modes, e.g., slow service, limited service, emergency service, etc. Here, we say that the system has suffered a partial failure of its functionality or performance.

Means for achieving dependability

- A combined use of methods can be applied as means for achieving dependability. These means can be classified into:

  1. **Fault Prevention techniques**

     to prevent the occurrence and introduction of faults

– design review, component screening, testing, quality control methods, ..

– formal methods

2. Fault Tolerance techniques

to provide a service complying with the specification in spite of faults

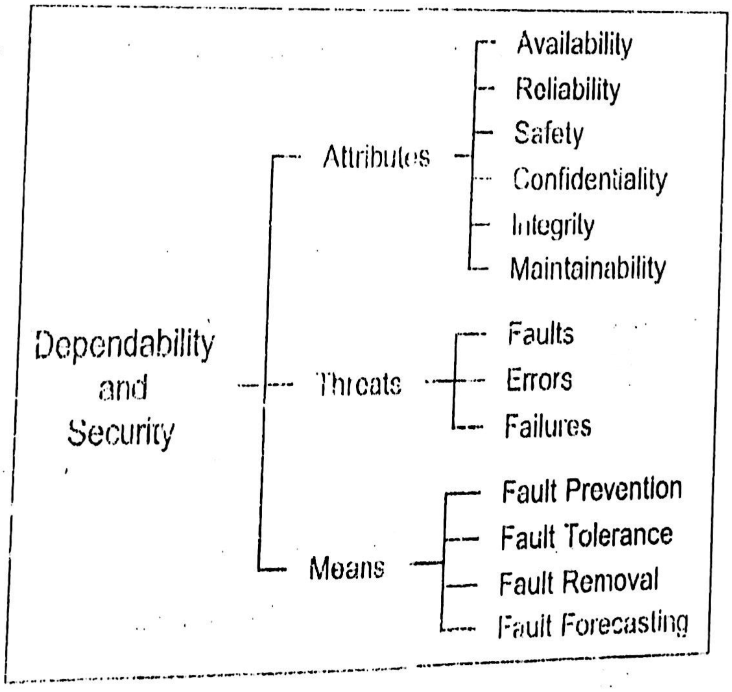
3. Fault Removal techniques

to reduce the presence of faults (number,seriouness, ...)

4. Fault Forecasting techniques

to estimate the present number, the future incidence, and the consequences of faults

Dependability tree



(*) Security: Availability, Confidentiality, Integrity

The Means to attain Dependability

1. **Fault prevention techniques**
2. **Fault tolerance techniques**
3. **Fault removal**
4. **Fault forecasting**

1. Fault prevention techniques

- Fault prevention techniques are intended to keep faults out of the system at the design stage

- Related to general system engineering techniques (design methodolgies, construction rules, use of high reliable components).
These include

  - a rigid software development process and
  formal methods

2. Fault tolerance techniques

Fault tolerance:

ability of the system to deliver a correct service after the occurrence of faults

- **Why fault tolerance techniques?**

even with the most careful fault avoidance, faults will eventually occur and result in a system failure

- **Fault tolerance techniques:**
carried out via error detection and system recovery, *redundancy* to counteract the effects of faults

Protective redundancy: additional components or processes that mask or correct errors or faults inside a system so they do not become observable failures in its service

Organisation of fault tolerance

Possible phases in response to fault manifestation

- Error detection
- Damage containment
- Damage assessment/diagnosis
- Reconfiguration
- Error recovery / restart
- Fault treatment / repair / reintegration

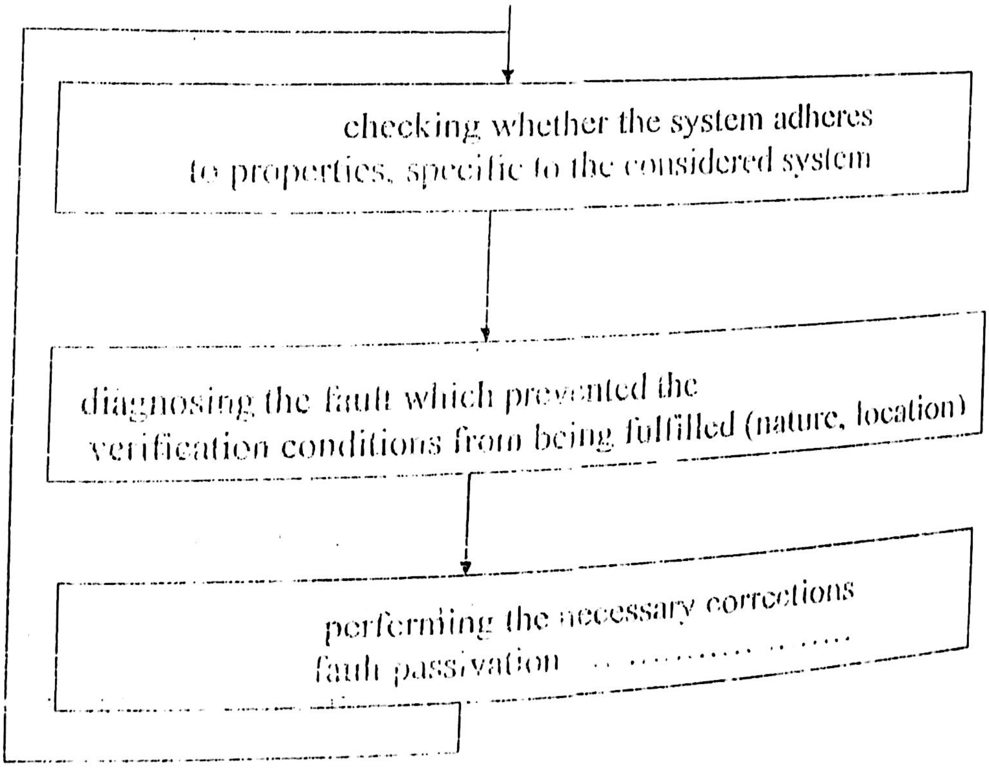
3. Fault removal techniques

➢ Fault diagnosis

- Nature and location of faults

➢ Fault passivation

- Removing the components identified faulty


checking whether the system adheres
to properties, specific to the considered system
diagnosing the fault which prevented the
verification conditions from being fulfilled (nature, location)
performing the necessary corrections
fault passivation .. ..

➢ **Important aspects:**